OLL 85-2725

Office of Legislative Liaison
Routing Slip

TO:	ACTION	INFO
1. D/OLL		X
2. DD/OLL		X
3. Admin Officer		
4. Liaison		X
5. Legislation	X	
6.		X
7.		
8.		
9.		
10.		

SUSPENSE ~~17 Sept 1985~~ (NOON)
Date

Action Officer:

Remarks:

~~BG / 16 Sept 1985~~
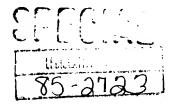**Name/Date**

STAT

STAT

STAT

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 16, 1985

LEGISLATIVE REFERRAL MEMORANDUM

85-2723

Chro

TO: Legislative Liaison Officer

Department of Commerce - Mike Levitt (377-3151)

General Services Administration - Ted Ebert (566-1250)

Central Intelligence Agency

SUBJECT: DOD testimony on H.R. 2889, the "Computer Security Research and Training Act of 1985"

The Office of Management and Budget requests the views of your agency on the above subject before advising on its relationship to the program of the President, in accordance with OMB Circular A-19.

A response to this request for your views is needed no later than

NOON, TUESDAY, SEPTEMBER 17, 1985

Questions should be referred to Constance J. Bowers (395-3457), the legislative analyst in this office.

James C. Murr for
Assistant Director for
Legislative Reference

Enclosures
cc: Ed Springer   Kevin Sheid   Russ Neely

STATEMENT

BY

DONALD C. LATHAM

ASSISTANT SECRETARY OF DEFENSE

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

AND

CHAIRMAN

NATIONAL TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY

COMMITTEE

CONCERNING H.R. 2889

BEFORE THE

SUBCOMMITTEE

ON LEGISLATION AND NATIONAL SECURITY

COMMITTEE ON GOVERNMENT OPERATIONS

UNITED STATES HOUSE OF REPRESENTATIVES

SEPTEMBER 18, 1985

Mr. Chairman and members of the Subcommittee:

Thank you for this opportunity to testify on H.R. 2889, known as the "Computer Security Research and Training Act of 1985". This bill has the objectives of providing for a computer security research program within the National Bureau of Standards (NBS) and also providing for the training of Federal Employees who are involved in the management, operation, and use of automated information (AIS) systems. The efforts of this subcommittee are to be applauded as it carries out in its investigation of the importance of the computer systems security problem to this nation and considers actions aimed at coming up with comprehensive remedies to this complex issue.

Today, I would like to address myself first to the general intent and overall purpose of the bill by providing perspectives, in my dual roles as both the Assistant Secretary of Defense for Command, Control and Communications and Chairman, National Tele-communications and Information Systems Security Committee (NTISSC), of the problems we face. Second, I would like to highlight possible areas of potential confusion in the bill requiring clarification so as not to impact adversely on existing Administration programs. Finally, I have included in my testimony suggested revisions to the bill for your careful review and action.

First, I wholeheartedly support the general intent of H.R. 2889 to provide for much needed support in the area of computer systems security training and education. All to often this is an area sorely overlooked and poorly funded because it is not glamorous. Also, as you are all too aware, the computer system security problem is extremely complex and solutions to the problem are made all the more difficult by continuing rapid advances in the state-of-the-art. The emerging use of supercomputers and the proliferation of local area networks are but two examples of technology that make the computer systems security problem a challenge that must be faced now. The problem is immense in scope and associated R&D in the area is totally inadequate. The shortage of highly qualified and trained professionals in computer systems security aggravates the problem. Any effort to try to assist in this endeavor is clearly welcome.

In this regard, I view H.R. 2889 as a positive step to achieve consensus on the need for additional resources. The National Bureau of Standards has for some time been an important center of expertise in certain facets of computer systems security. It is entirely appropriate, therefore, that the NBS be tapped to take on additional responsibilities and funding in research and related activities as reiterated in the Bill. Let me quickly caveat my comments by saying that, to be truly effective, these additional NBS efforts must be further focused in the context of on-going efforts such as those which fall under National Security Decision Directive (NSDD-145) so to avoid costly duplication of effort. I will address this issue in some detail later.

As Chairman of the NTISSC, I view as one of my key responsibilities making sure the problem of computer systems security is recognized by the public at-large as an important national issue. We have not done as good a job as we might have done in the past because we were not properly organized. The NTISSC structure now in being provides that organization and we are moving ahead with an aggressive awareness program in concert with similar initiatives being carried out by the NBS.

At its last meeting on 4 September 1985, the Subcommittee on Automated Information Systems security (SAISS), one of the two major subcommittees of the NTISSC, approved for issuance to the NTISSC a proposal to require education and training of federal departments and agencies. I expect the NTISSC to take up this proposal and make it a National Policy. In this regard, the National Computer Security Center (NCSC) at the National Security Agency (NSA) has begun development of training courses in AIS systems security for a DoD-sponsored awareness program. The NCSC will provide materials to other government, departments and agencies for awareness training. Of course, funding for such training resources remains a problem.

Let me focus just a moment on some other DoD education and training efforts. We are developing guidelines which will make it easier to determine and specify the level of security that a system needs when generating requests for procurements or acquisitions. Also, we are in the process of issuing a Standard entitled, "DoD Trusted Computer System Evaluation Criteria", hereafter referred to as the Criteria, to assist in evaluating the effectiveness of safeguards for Defense applications. By the way, the SAISS adopted use of the Criteria on an interim one-year trial basis. Finally, the DoD is undertaking an ambitious computer vulnerability reporting program aimed at correcting security weaknesses in DoD computer systems. This effort should also be very useful for designing a national reporting program.

In my testimony for Mr. Glickman, Chairman of the Subcommittee on Transportation, Aviation and Materials, Committee on Science and Technology, on 27 June 1985, I indicated that a high priority item was trying to provide a working definition for what constitutes "sensitive" information. Since that time, the SAISS has approved for issuance to the NTISSC a proposal for defining sensitive information. Specifically, it separates unclassified but sensitive information into two categories: sensitive national security-related; and sensitive non-national security-related. The purview of NSDD 145 is only for the former category. Unclassified but sensitive non-national security-related is the concern of the civilian sector with NBS playing a major role.

Let me reiterate that NSDD-145 does not cover unclassified but sensitive non-national security-related information and therefore, it in no way restricts, controls, or manages the activities of other federal departments or agencies who have responsibilities in non-national security-related areas. In order to maintain this clear

demarcation line, language in H.R. 2889 making reference to "sensitive" information should be amended to reflect that "unclassified but sensitive non-national security-related" data is the subject data in question.

On the matter of research and development (R&D) responsibilities, the NBS has a well-developed program in the area of computer systems security. The NBS derives its responsibilities from the Brooks Act of 1965 (P.L. 89-306), , the Privacy Act of 1974 (P.L. 93-579), and the Paperwork Reduction Act of 1980 (P.L. 96-511). We view these responsibilities as distinct both in intent and focus from those cited in NSDD-145. Again, NSDD-145 addresses only unclassified but sensitive national security-related and does not cover unclassified but sensitive non-national security-related information. More directly, privacy information, information on fraud, waste, and abuse, or proprietary data held by an agency is not covered by NSDD-145 dictates.

Let me quickly add that we don't intend to meddle in NBS authorities or responsibilities in these areas. Rather, we see the NBS efforts and those of other federal agencies under NSDD-145 as complementary and supportive of each other. Clearly, technical measures and techniques can apply equally well in many circumstances and technical interaction must be encouraged.

Indicative of the strong current relationship between the NBS and the DoD, is the high-level of cooperation between the NBS and the National Computer Security Center at NSA which is already impressive and growing. Specifically, they have jointly sponsored for the past eight years a National Computer Security Conference. This year's conference, scheduled from 29 September 1985 to 3 October 1985, will focus on mutual subjects of concern such as secure networks, verification, labelling, a profile of "hackers", and data base management security to name just a few. It will be attended by business, academia and government and allows for critical transfer of the results of the National Computer Security Center research and the NBS research throughout government and the private sector.

Important work is proceeding between NBS and the NCSC in the area of personal computers and office automation. In this regard, a Guideline on Password Management is being published by the NCSC and will become an appendix to the NBS Password Usage Standard already in existence. Additionally, the NBS has done impressive work in micro-computer and mini-computer systems security which the NCSC is using. As a final example, NBS and the NCSC is sponsoring a symposium on risk analysis to examine methodologies of mutual benefit. Again, these efforts represent the high degree of interaction between these two centers of expertise.

This cooperation must continue. However, the federal audiences for their respective services is different. The NCSC's target audience is the National Security Community while NBS services the

civilian sector. While the staffs of both organizations are highly specialized, there is continuing reliance by NCSC staff on NBS Institute for Computer Sciences and Technology (ICST) staff expertise and vice-versa. In fact, two NSA employees currently are working at NBS with the purpose of transfering expertise to civilian users. This arrangement has worked remarkably well in the past and must be preserved.

Let me add that the NBS has taken an active role in the Subcommittee on Automated Information Systems Security (SAISS) of the NTISSC. The NBS member is the ICST Director, Mr. James Burrows. Mr. Burrows has been instrumental in the promulgation by the SAISS of the recent issuance relating to defining sensitive information categories as well as the issuance on training and education.

As a final point on the issue of NSDD-145 and NBS responsibilities, NSDD-145 requires that NBS submit for NTISSC approval proposed computer systems security standards prior to their issuance as a Federal Information Processing System (FIPS) standard. Once again, this applies only to proposed standards where national security-related matters are concerned Standards unrelated to national security are not covered. In this regard, it is anticipated that, Federal Information Processing Standard No. 112, Password Usage Standards, , will be the first such standard processed under the NTISSC structure because it has application to both both unclassified and classified processing environments.

In accordance with the preceding, I would now like to turn my attention to some of the areas in the bill that potentially could cause confusion and which, I feel, could benefit from additional clarification.

First, on page 2 of H.R. 2889, reference is made to "sensitive" information. I suggest this be amended to read "sensitive unclassified non-national security-related." Also, for clarity, this phrase should also be used to modify the use of the term "information" as used on page 3 Sec. 18 (b) (2).

Second, on page 3 of H.R. 2889, Section 18 (a) should be amended to clearly set forth that H.R. 2889 does not seek to impact Administration efforts under NSDD-145. Therefore, I propose the following be inserted as the last sentence of paragraph (c): "The following NBS program shall be undertaken in consonance with those computer system security responsibilities delineated in National Security Decision Directive 145, "National Policy on Telecommunications and Automated Information System Security." This important adjustment minimizes overlap of responsibilities between the Department of Commerce and the Department of Defense and recognizes that both programs are complementary and supportive.

In closing, let me allay the fears of those who feel that NSDD-145 does in some way, shape, or form restrict current NBS

research and development for standards-making efforts. NSDD-145 and the NBS programs stemming from the statutory base already mentioned are compatible and complementary efforts.

Computer systems security is a major challenge that needs all the available brainpower and resources this nation can muster. As such, let's move ahead together in the spirit of harmony and cooperation, not competition. I feel H.R. 2889, with the recommended changes I proposed, is a positive step in fostering this spirit of cooperation.

Accompanying me is Mr. Robert Rich, Deputy Director, NSA, who will further describe the activities of the Computer Security Center and other programs now being carried out by NSA in the areas of computer systems security awareness, education, training, and research and development.

Mr. Chairman, this concludes my prepared remarks. I would be happy to answer any questions that you or the Subcommittee have.